



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/982,624	10/18/2001	Taizo Shirai	450100-03550	8604

20999 7590 09/23/2005

FROMMER LAWRENCE & HAUG
745 FIFTH AVENUE- 10TH FL.
NEW YORK, NY 10151

EXAMINER

PARTHASARATHY, PRAMILA

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 09/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/982,624

Applicant(s)

SHIRAI ET AL.

Examiner

Pramila Parthasarathy

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 July 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-9 is/are pending in the application.
- 4a) Of the above claim(s) 5 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4 and 6-9 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This action is in response to request for reconsideration filed on July 05, 2005. Original application contained Claims 1 – 9. Applicant has canceled claims 5. Applicant has amended claims 1, 6, 7, 8 and 9. Claims are 1 – 4 and 6 – 9 are pending.

Response to Arguments

2. Applicant's arguments with respect to claims 1 – 4 and 6 – 9 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 1 – 4 and 6 – 9 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The amended independent Claims 1 and 6 – 8 read, “ ... said CBC mode encrypts said data using said set of keys based on at least one of the sectors of said data encrypted by said integrity-check-value generating key”.

With respect to “CBC mode encrypts said data using said set of keys based on at least one of the sectors of said data encrypted by said integrity-check-value generating key”, although the specification discloses “... an integrity-check-value generating key of data to be stored in at least one of the sectors.” and “In the cryptosystem unit, the received set of keys may be encrypted in the CBC mode and are transmitted to the device.”, the specification does not disclose “CBC mode encrypts said data using said set of keys based on at least one of the sectors of said data encrypted by said integrity-check-value generating key”. Applicant amendment does not clarify the steps of “CBC mode encrypts said data using said set of keys based on at least one of the sectors of said data encrypted by said integrity-check-value generating key”, and does not direct to specific location to specification for disclosing CBC mode encrypts said data using said set of keys based on at least one of the sectors of said data encrypted by said integrity-check-value generating key.

The dependent claims 2 – 4 are rejected at least by virtue of their dependency on the dependent claims.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1 – 4 and 6 – 9 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Bellare et al. (U.S. Patent Number 5,673,319).
6. Regarding Claim 1, Bellare teaches and describes a data storage area consisting of a plurality of blocks, each of which consists of a plurality of sectors which each have a predetermined data capacity (Summary and Column 5 lines 5 – 21); and
cryptosystem means (Summary and Column 5 lines 5 – 21);
wherein said cryptosystem means receives, as cryptosystem keys for performing cryptosystem processing on data to be stored in said data storage area a set of keys correlated with the encryption keys or decryption keys for each of the sectors from a device capable of performing data communication with said data storage device and an integrity-check-value generating key of data to be stored in at least one of the sectors, and transmits, to said device, a set of encrypted keys obtained by executing encryption processing in the cipher block chaining (CBC) mode on the received set of keys; said CBC mode encrypts said data using said set of keys based on at least one of the sectors of said data encrypted by said integrity-check-value generating key (Summary and Column 5 line 5 – Column 6 line 35).

7. Regarding Claim 6, Bellare teaches and describes executing mutual authentication processing between said data storage device and said data recording device (Summary and Column 5 lines 5 – 21);

when the mutual authentication is established, transmitting, to said data storage device, by said data recording device, a set of session-key-used CBC-mode-processing keys which are generated by executing, based on a session key generated in the mutual authentication, encryption processing in the CBC mode on said set of keys applicable to encryption processing on pieces of data to be stored in the sectors and an integrity-check-value generating key of data to be stored in at least one of the sectors, said CBC mode encrypts said data using said set of keys based on at least one of the sectors of said data encrypted by said integrity-check-value generating key (Summary and Column 5 lines 5 – 21);

decrypting, by said data storage device, said set of session-key-used CBC-mode-processing keys by performing decryption in the CBC mode using the session key (Summary and Column 5 lines 22 – 34);

transmitting, to said data storage device, a set of decrypting, by storage-key-used generated by executing based on a storage key unique to said data storage device, encryption processing in the CBC mode on the set of decrypted session-key-used CBC-mode-processing keys (Summary and Column 5 line 5 – Column 6 line 35);
and

generating, by said data recording device, header information including as a component the received set of storage-key-used CBC-mode-processing keys which are

Art Unit: 2136

generating, by said data recording device, header information including as a component the received set of storage-key-used CBC-mode-processing keys, the header information corresponding to the data to be stored in said data storage device (Summary and Column 5 line 5 – Column 6 line 35).

8. Regarding Claim 7, Bellare teaches and describes executing mutual authentication processing between said data storage device and said data playback device (Summary and Column 5 lines 5 – 21);

when the mutual authentication is established, transmitting, from said data playback device to said data storage device, a set of storage-key-used CBC-mode-processing keys which is included in the header information of data stored in said data storage area and which is generated by executing encryption processing in the CBC mode using a storage key unique to said data storage device and an integrity-check-value generating key of data to be stored in at least one of the sectors, said CBC mode encrypts said data using said set of keys based on at least one of the sectors of said data encrypted by said integrity-check-value generating key (Summary and Column 5 lines 5 – 21);

decrypting, by said data storage device, the set of storage-key-used CBC-mode-processing keys by performing decryption in the CBC mode using the storage key (Summary and Column 5 lines 5 – 34);

transmitting, by said data storage device, to said data playback device, a set of session-key-used CBC-mode-processing keys which are generated by executing,

based on a session key generated in the mutual authentication encryption processing in the CBC mode on the set of decrypted storage-key-used CBC-mode-processing keys (Summary and Column 5 line 5 – Column 6 line 35); and

obtaining, by said data playback device, a set of keys for decrypting encrypted sector data which is stored in each of the sectors in said data storage area by decrypting, in the CBC mode, the session-key-used CBC-mode-processing keys by using the session key (Summary and Column 5 line 5 – Column 6 line 35).

9. Regarding Claim 8, Bellare teaches and describes executing mutual authentication processing between said data storage device and said data recording device (Summary and Column 5 lines 5 – 21);

when the mutual authentication is established, transmitting, to said data storage device, by said data recording device, a set of session-key-used CBC-mode-processing keys which are generated by executing, based on a session key generated in the mutual authentication, encryption processing in the CBC mode on said set of keys applicable to encryption processing on pieces of data to be stored in the sectors and an integrity-check-value generating key of data to be stored in at least one of the sectors, said CBC mode encrypts said data using said set of keys based on at least one of the sectors of said data encrypted by said integrity-check-value generating key (Summary and Column 5 lines 5 – 21);

decrypting, by said data storage device, said set of session-key-used CBC-mode-processing keys by performing decryption in the CBC mode using the session key (Summary and Column 5 lines 22 – 34);

transmitting to said data storage device, a set of storage-key-used CBC-mode-processing keys which are generated by executing, based on a storage key unique to said data storage device, encryption processing in the CBC mode on the set of decrypted session-key-used CBC-mode-processing keys (Summary and Column 5 line 5 – Column 6 line 35); and

generating, by said data recording device, header information including as a component the received set of storage-key-used CBC-mode-processing keys which are generating, by said data recording device, header information including as a component the received set of storage-key-used CBC-mode-processing keys, the header information corresponding to the data to be stored in said data storage device (Summary and Column 5 line 5 – Column 6 line 35).

10. Regarding Claim 9, Bellare teaches and describes executing mutual authentication processing between said data storage device and said data playback device (Summary and Column 5 lines 5 – 21);

when the mutual authentication is established, transmitting, from said data playback device to said data storage device, a set of storage-key-used CBC-mode-processing keys which is included in the header information of data stored in said generated by executing data storage area and which is encryption processing in the

Art Unit: 2136

CBC mode using a storage key unique to said data storage device and an integrity-check-value generating key of data to be stored in at least one of the sectors, said CBC mode encrypts said data using said set of keys based on at least one of the sectors of said data encrypted by said integrity-check-value generating key (Summary and Column 5 lines 5 – 21);

decrypting, by said data storage device, the set of storage-key-used CBC-mode-processing keys by performing decryption in the CBC mode using the storage key (Summary and Column 5 lines 22 – 34);

transmitting, by said data storage device, to said data playback device, a set of session-key-used CBC-mode-processing keys which are generated by executing, based on a session key generated in the mutual authentication, encryption processing in the CBC mode on the set of decrypted storage-key-used CBC-mode-processing keys (Summary and Column 5 line 5 – Column 6 line 35); and

obtaining, by said data playback device, a set of keys for decrypting encrypted sector data which is stored in each of the sectors in said data storage area by decrypting, in the CBC mode, the session-key-used CBC-mode-processing keys by using the session key (Summary and Column 5 line 5 – Column 6 line 35).

11. Claim 2 is rejected applied as above in rejecting Claim 1. Furthermore, Bellare teaches and describes wherein said cryptosystem means, generates key data as the header information of the data to be stored in said data storage area by using a storage key which is unique to said data storage device to execute the encryption processing in

Art Unit: 2136

the CBC mode on the received set of keys (Summary and Column 5 line 5 – Column 6 line 35).

12. Claim 3 is rejected applied as above in rejecting Claim 1. Furthermore, Bellare teaches and describes said data storage with said device capable of performing data communication with said data storage device (Summary and Column 5 lines 5 – 21);

the received set of keys is a set device performs mutual authentication of session-key-used CBC-mode-processing keys a session key generated in the mutual authentication (Summary and Column 5 lines 5 – 21);

said cryptosystem means performs the decryption in the CBC mode of said set of encrypted session-key-used CBC-mode-encrypted in the CBC mode by using processing keys (Summary and Column 5 lines 22 – 34); and

in said cryptosystem means CBC-mode-processing keys is generated by executing, based on a storage key unique to said data storage device, the encryption processing in the CBC mode on the set of decrypted session-key-used CBC-mode-processing keys, and said set of storage-key-used CBC-mode-processing keys is a set of storage-key-used transmitted as header-information-forming data to said device (Summary and Column 5 line 5 – Column 6 line 35).

13. Claim 4 is rejected applied as above in rejecting Claim 1. Furthermore, Bellare teaches and describes said data storage device performs mutual authentication with said device capable of performing data communication with said data storage device;

the received set of keys is header information on the data to be stored in said data storage area, and is a set of storage-key-used CBC-mode-processing keys encrypted in the CBC mode based on a storage key unique to said data storage device (Summary and Column 5 lines 5 – 21);

said cryptosystem means performs the decryption in the CBC mode of the set of encrypted storage-key-used CBC-mode-processing keys by using said storage key (Summary and Column 5 lines 22 – 34); and

in said cryptosystem means, a set of session-key-used CBC-mode-processing keys is generated by executing, based on a session key generated in the mutual authentication, the encryption processing in the CBC mode, and said set of session-key-used CBC-mode-processing keys is transmitted as data constituting decrypting key information (Summary and Column 5 line 5 – Column 6 line 35).

Conclusion

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

15. Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant.

Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

16. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

Art Unit: 2136

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
September 18, 2005.


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100